SET A STRONG PASSWORD

Use an acronym to create a sentence from your password e.g. t2cmlp,@yh (“Try to crack my latest password, all you hackers”) or use a password manager such as 1password or Yoti.
USE TWO-STEP AUTHENTICATION

On all your social media or email accounts - a code will be sent to your phone through a text or an app whenever you or someone else tries to log in from an unfamiliar browser. You can turn this on from your security settings.
DO REGULAR PRIVACY HEALTH CHECKS

Every 3 months go through the privacy settings on your social media accounts - are you happy with who can see your content?
HIDE YOUR LOCATION

Turn off your location settings and don’t check in on social media whilst you’re still there. Tag the location only after you have left.
CLEAN UP YOUR SOCIAL MEDIA HISTORY

What groups are you a part of? Are you happy to be a part of them? Are you happy with the information you’ve made public in the past? Who are you following? Do you still want to be following them?
CHECK IF YOUR DATA HAS BEEN BREACHED

Use haveibeenpwned.com to see if your personal data has ever been released.
Digital Self-Care is about identifying, communicating and respecting boundaries in your online spaces.
CREATE ONLINE BOUNDARIES

Use a pinned post explaining what you will or won’t engage with online. Use the block and report functions when needed!

Pin to the top of my page

Block this account
SPEND SOME TIME OFFLINE

Take breaks from social media during stressful moments and do something you enjoy.

Remove app
Talk to your friends and family about online abuse, let them know how they can support you and reach out if you need someone to talk to.
- Online Abuse 101
- Documenting Online Abuse Form
- Your Digital Resilience Action Plan
- Online Chatbot